Integrantes: Caroline Jenuario Rodrigues da Silva

O primeiro passo foi implementar um programa para armazenar senhas e nomes de 4 caracteres em um arquivo em formato txt. Para armazenar as senhas, foi utilizado o algoritmo MD5 para criptografar os valores reais, que é caracterizado por ser uma função hash, produzindo um valor de hash de 128 bits expresso em 32 caracteres. Tal algoritmo é usado por softwares com protocolo ponto-a-ponto (P2P) e como uma soma de verificação para checar a integridade de dados, mas apenas contra corrupção não intencional.

No segundo passo, em posse do arquivo txt contendo as senhas criptografadas, foi utilizado um programa que realiza um algoritmo de ataque de força bruta que consiste em uma tentativa de violar uma senha ou um nome de usuário, descobrir uma chave usada para criptografar uma mensagem, usando uma abordagem de tentativa e erro. Em seguida, foi realizado testes com 4 das senhas armazenadas no arquivo txt, e a média de tempo para o programa realizar a quebra da criptografia e encontrar o valor real da senha foi 55ms. Portanto, pode se concluir que o algoritmo possui vulnerabilidades, já que a mensagem original foi facilmente decifrada. Ademais, ele pode ser adequado para outros fins não criptográficos como para determinar a partição para uma chave específica em um banco de dados particionado.

No terceiro passo, para minimizar os problemas relacionados a quebra de criptografia, o programa foi modificado, e o algoritmo SHA-256 foi implementado no lugar no MD5. Este algoritmo são funções hash computadas com palavras de 32 bytes, o qual tem como objetivo criar hashes ou códigos exclusivos com base em um padrão com dados do computador possam ser protegidos contra qualquer agente externo que deseje mudá-los. Portanto, esse algoritmo não pode ser quebrado, e é um grande avanço para garantir a privacidade do conteúdo no processamento de informações, resolvendo os problemas relacionados a vulnerabilidades encontradas no MD5. Além disso, o programa foi modificado para limitar o tempo de acesso para no máximo 50000 ms, para que assim, o usuário não consiga realizar inúmeras tentativas de obter a senha.